IDG.net

Linux listens for the federal buzz SEE PAGE 44

Federal Computer Week

JANUARY 25, 1999 *The Newspaper for Federal IT Decision-Makers* VOLUME 13 NUMBER 2

First Look: We test drive Panasonic's rugged Toughbook 27. Page 33

Air Force lab develops tech to secure digital imagery

BY DANIEL VERTON

The Air Force Research Laboratory, Rome, N.Y., has developed a cutting-edge technology solution that aims to boost Internet security by preventing the fraudulent manipulation of photographs, videos and other digital media used throughout government and industry.

The technology, known as digital watermarking, ensures the security and authentication of digital photographs by embedding an encrypted image over the original photograph, like the watermarks used to ensure the authenticity of the new $20, $50 and $100 bills.

According to Air Force officials, the technology will prevent hackers and foreign intelligence agents from altering sensitive or classified digital imagery or videos that are transmitted over the Internet. The technology also can be used to prevent fraudulent reproductions of commercial music and video CDs.

"This process falls under [the discipline] of steganography, [or] the art of hiding a secret message in an innocuous carrier," said Lt. Arnold Baldoza, technical director for the research project. "For example, one can hide a classified image in a digital family portrait."

Digital watermark technology holds significant implications for military and commercial security and anti-fraud applications. For example, embedding data in digital media may be the solution to problems such as widespread copyright violations, illegal copying and distribution of compact discs and CD-ROMs, and easy forging of digital videos and photographs.

"Digital watermarks, if designed properly, can be used as proof of ownership, as a content authentication tool [for tampering detection] and as a means of imprinting source identification information into the image" to ensure the integrity of the source, Baldoza said.

The new technology will help the Air Force secure the transmission of intelligence information, he said. "We envision the Air Force using this technology to embed additional information into [intelligence] imagery...[and] to detect unauthorized tampering of its imagery," Baldoza said. "Since digital watermarks are embed-

See **AIR FORCE**, *Page* **19**

Air Force

FROM *Page* **18**

ded directly into and are inseparable from their carrier, this additional information would always be available with the image."

The encrypted pattern or image is generated by a pseudo-random number generator and then smoothed, or polished, before being embedded. If a hacker modifies the image, he affects the watermark. And if the watermark is generated based on a cryptographically strong key, a hacker would not be able to calculate and embed a new watermark, Baldoza said.

Jiri Fridrich, a professor at the State University of New York, Binghamton, N.Y., who helped the Air Force develop its initial R&D effort in this area called "Secure Image Ciphering based on Chaos," said digital watermarks overcome some of the limitations of traditional ciphering methods, which use mathematical calculations to produce authentication keys.

Classical digital signatures are "just for exchange of data and cannot be used for protecting the digital data after decryption," Fridrich said. "Once an image is decrypted and posted on a Web page [or] shown on a TV monitor, there is no further protection of the data. This is when watermarking and data hiding comes into place."

However, Bill Malik, vice president and research director of the research firm Gartner Group, said the establishment of a third-party testing and evaluation body is key to the widespread acceptance of digital watermark technology, particularly from a legal standpoint. The main question surrounding this technology is "how do you certify its strength?" Malik said. In addition, it is important to ask, "Do you have a legal system that is willing to accept that level of strength" when you bring it to court?

Air Force researchers first envisioned the project in 1997 when they began work on a Small Business Innovative Research project known as "Secure Encryption and Hiding of Intelligence Data." The goal of the initial project was to develop a secure and efficient method of transmitting digital data using the Internet and other media. The SBIR effort is now in Phase Two and is scheduled for completion in March 2000.

Although the SBIR program rarely funds Phase Three efforts — the commercialization phase of developing a new product — Baldoza said the Air Force is pursuing alternative sources of funding as well as a dual-use contract with a major commercial company to help develop products that use digital watermark technology. "If the contract is awarded, we might see this technology become available to the general public in two to three years," Baldoza said.

The Air Force's solution for digital watermarking is quickly becoming "old" by development standards, Fridrich said, but he still believes the Air Force project is an important step in the right direction, particularly for early adopters of digital money and online product distribution. "It's absolutely necessary" for the future, he said. ■